McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

October 27, 2020

VIA U.S. MAIL AND EMAIL(ndaq@nd.gov)

North Dakota Attorney General
Office of Consumer Protection
600 E. Boulevard Ave Dept. 125
Bismarck ND 58505

Re: State of North Dakota – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents the State of North Dakota ("North Dakota"). I am writing to provide notification of an incident at North Dakota that may affect the security of personal and/or protected health information of twenty five thousand, five hundred and eighty-six (25,586) North Dakota residents. North Dakota's investigation is ongoing and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any.

After a series of phishing incidents, an unauthorized party obtained access to several employee email accounts. Upon learning of the issue, North Dakota contained the accounts and commenced a prompt and thorough investigation. As part of the investigation, North Dakota worked closely with external cybersecurity professionals. After an extensive and very comprehensive forensic investigation and manual document review, North Dakota discovered on August 27, 2020 that the email accounts that were accessed between November 23 and December 23, 2019 contained some of the residents personal and/or health information. The information included the residents' date of birth, medical diagnosis/medical treatment information, Social Security number, driver's license or state identification number, passport number, digitized or electronic signature, financial account number, and credit or debit card number. Not all information was included for all residents.

North Dakota's investigation is ongoing. Nevertheless, out of an abundance of caution, North Dakota wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. North Dakota will provide the affected residents with written notification of this incident commencing on or about October 27, 2020 in substantially the same form as the letter attached hereto. The affected residents are being provided with advice on steps they can take to prevent medical identity theft. North Dakota is providing the residents who had their Social Security number included in the accessed account with twelve (12) months of credit monitoring. North Dakota is advising the affected

residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. North Dakota is also advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Protecting the privacy of personal information is a top priority. North Dakota remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. North Dakota continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Notice is being provided pursuant to the HIPAA Breach Notification Rule, 45 CFR §§ 164.400, *et seq.*

Should you have any questions regarding this notification, please contact me at (248)-220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,

James J. Giszczak

Encl.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

[redacted]

Dear [redacted]:

I am writing with important information regarding a recent data security incident. The privacy and security of the personal information we maintain is of the utmost importance to the State of North Dakota. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

As a result of a series of phishing incidents, an unauthorized party obtained access to several employee email accounts. The accessed accounts were limited to the Department of Health, the Department of Human Services, a local public health unit, and a few other state agencies. The incident did not impact State of North Dakota servers and/or systems and was limited to certain employee email accounts only.

What We Are Doing.

Upon learning of this issue, we contained the accounts and commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an extensive and very comprehensive forensic investigation and manual document review, we discovered on August 27, 2020 that the email accounts that were accessed between November 23 and December 23, 2019 contained some of your personal and/or health information. **We have no evidence that any of your information was acquired or used by the unauthorized party.**

Since the date of this incident, we have taken significant measures to mitigate the recurrence of similar incidents in the future, including reviewing and revising policies and procedures as needed and providing additional education to our workforce members on identifying and responding to a phishing attack.

What Information Was Involved?

The email accounts that were accessed contained some of your personal and/or protected health information, specifically your [redacted]

What You Can Do.

We have no evidence that any of your information was acquired or used by the unauthorized party. Nevertheless, out of an abundance of caution and to protect you from potential misuse of your information, we are offering you a one-year membership in myTrueIdentity provided by TransUnion Interactive, a subsidiary of TransUnion. For more information on identity theft prevention and myTrueIdentity, including instructions on how to activate your one-year membership, please see the additional information provided in this letter.

This letter also provides you with precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. We are also offering steps you can take to protect your medical information on the following pages.

For More Information.

We regret any inconvenience that this may cause you. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to secure personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 am to 9 pm Eastern Time.

Sincerely,

Risk Management Division
State of North Dakota

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

You can sign up for the online credit monitoring service anytime between now and [redacted]. Due to privacy laws, we cannot register you directly. Please note that credit monitoring service might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you believe you may be a victim of identity theft, please call the toll-free TransUnion Fraud Response Services hotline at [redacted]. When prompted, enter the following 6-digit telephone pass code [redacted] to speak to a TransUnion representative about your identity theft issue.

Special note for minors affected by this incident: The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security Number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial one (1) year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-349-9960

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

6. Protecting Your Medical Information.

We have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164.